October 8, 2018

The Honorable John Thune
Chairman
Committee on Commerce, Science
and Transportation
512 Dirksen Senate Building
Washington, D.C. 20510

The Honorable Greg Walden
Chairman
Committee on Energy
and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Ben Nelson
Ranking Member
Committee on Commerce, Science
and Transportation
512 Dirksen Senate Building
Washington, D.C. 20510

The Honorable Frank Pallone
Ranking Member
Committee on Energy
and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairmen and Ranking Members:

In light of your important leadership roles in Congress, we want to assure you that a recent report in Bloomberg Businessweek alleging the compromise of our servers is not true. You should know that Bloomberg provided us with no evidence to substantiate their claims and our internal investigations concluded their claims were simply wrong.

We are eager to share the facts in this matter because, were this story true, it would rightly raise grave concerns. A compromise of this magnitude, and the effective deployment of malicious chips like the one described by Bloomberg, would represent a serious threat to the security of systems at Apple and elsewhere. That's why, ever since we were first contacted by Bloomberg's reporters in October 2017, we have worked diligently to get to the bottom of their allegations.

While the story was being reported, we spoke with Bloomberg's reporters and editors and answered any and all of their questions. We methodically dispelled the often-shifting nature of their claims. While we repeatedly asked them to share specific details about the alleged malicious chips that they seemed certain existed, they were unwilling or unable to provide anything more than vague secondhand accounts.

We were struck by the fact that the gravity and magnitude of the claims seemed to be undermined by their uncertainty around key details. Nevertheless, we worked tirelessly

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275
www.apple.com

to ascertain whether these claims were true or, failing that, if anything even like them were true.

In the end, our internal investigations directly contradict every consequential assertion made in the article—some of which, we note, were based on a single anonymous source.

Apple has never found malicious chips, “hardware manipulations” or vulnerabilities purposely planted in any server. We never alerted the FBI to any security concerns like those described in the article, nor has the FBI ever contacted us about such an investigation.

On Saturday night, the U.S. Department of Homeland Security joined the U.K.’s National Cyber Security Centre in saying they have no reason to doubt the statements we’ve made.

Our frustration is animated by the fact that we share your rightful focus on cybersecurity and the integrity of the global supply chain. We understand that, though this story only relates to our enterprise hardware, Americans are justly concerned about how supply chain security affects the consumer products they use every day. Concern for supply chain security is absolutely central to the way we run our business.

If any of the reported details cited above were true, we would have every interest—economic, regulatory, and ethical—to be forthcoming about it. We hold ourselves to the highest standard in the products we create and the data we safeguard, and to help address any concerns you may have, I would like to offer a brief summary of the supply chain protocols we follow to protect ourselves and our customers.

With respect to the information systems we use, we purposely work with multiple vendors, and our infrastructure is very diverse, protected by multiple layers of security. We deploy both commercially available and Apple proprietary security tools, led by an experienced security team that is familiar with diverse threats, simple and sophisticated.

We apply rigorous and ongoing diligence to vendors. Before we begin a relationship, vendors are submitted to a review process which can incorporate, depending on the criticality of the services offered, a layers-deep study of the security infrastructure of the vendor in question. The hardware incorporated into our environment is also placed in

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275
www.apple.com

the scope of Apple's Vulnerability Management Program which makes these products subject to ongoing vulnerability scans, patching, and security reviews.

In the situation Bloomberg describes, the so-called compromised servers were allegedly making outbound connections. Apple's proprietary security tools are continuously scanning for precisely this kind of outbound traffic, as it indicates the existence of malware or other malicious activity. Nothing was ever found.

I understand that these topics are of particular interest to your committees. I will be available to brief your staff this week to further address the information we've offered here.

Today, individuals, communities, and nations depend on the security and integrity of our shared technological infrastructure. We at Apple hold this responsibility sacrosanct, and we will continue to dedicate intense focus on keeping ahead of the hackers, cybercriminals, and even nation states that hope to steal data and harm user faith in the potential of technology to build a better world.

Sincerely,

George Stathakopoulos
Vice President, Information Security

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275
www.apple.com